AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of preventing falsification of an image produced in an imaging apparatus, comprising the steps of:

extracting a first image characteristic amount from said produced image in said imaging apparatus, by using one ~~randomly selected~~ specified algorithm ~~from of a plurality of algorithms in each photographing session~~;

recording identification information of said produced image in said imaging apparatus, ~~and~~ said first image characteristic amount and one specified algorithm or information thereof into a database of an authentication section which authenticates a status that there is no falsification in said produced image;

requesting authentication of an object image to said authentication section, to which identification information is provided;

reading out said first image characteristic amount and said one specified algorithm or said information thereof recorded together with said identification information of said produced image which is the same as said identification information of said object image from said database in said authentication section;

extracting a second image characteristic amount from said object image by using said ~~randomly selected~~ one specified algorithm read out from said ~~object image~~ database;

comparing said first image characteristic amount read out from said database with said second image characteristic amount~~, in which said extracted authentication data and said authentication data recorded in said database have the same identification information~~ extracted from said object image; and

judging whether or not said object image is falsified after said image production, based on consistency between said first and second image characteristic amounts acquired from said comparison in order to prevent said falsification of said produced image based on said judgment.

2. (previously presented) The method according to claim 1, wherein said imaging apparatus has a camera, in which said produced image is a photographic image photographed by said camera, in which said identification information is at least an identification information of a file name of said photographic image or an identification information for a photographer of said photographic image.

3. (previously presented) The method according to claim 1, wherein said imaging apparatus has a computer in which said produced image is a computer graphics image produced by said computer or an image which has been image-processed by said computer, and said identification information is at least an identification information of a file name of said produced image, or an identification information of a producer of said produced image.

4. (currently amended) A method of preventing falsification of an image produced in an imaging apparatus, comprising the steps of:

producing ~~an~~ said image to acquire a first image data of the produced image~~,~~;

recording identification information for identifying said produced image and said first image data of said produced image into a database in an authentication section which authenticates that there is no falsification in said produced image~~,~~;

requesting authentication of an authentication object image to said authentication section, to which identification information is provided;

reading out said first image data recorded together with said identification information of said produced image which is the same as said identification information of said authentication object image from said database in said authentication section;

acquiring a second image data from said authentication object image;

comparing an ~~extracted~~ acquired second image data of ~~an~~ said authentication object image which has been requested to be authenticated by said authentication section, with said first image data ~~recorded in~~ read out from said database~~,~~ in ~~the~~ said authentication section~~;~~

~~in which said extracted authentication data and said authentication data recorded in said database have the same identification information,~~

and

judging whether or not said authentication object image is falsified after said image production, based on a consistency between said first and second image data acquired from said comparison in order to prevent said falsification of said produced image based on said judgment~~,~~

~~wherein when looking at the consistencythe exact matching between the data is not required~~.

5. (previously presented) The method according to claim 4, wherein said imaging apparatus has a camera, in which said produced image is a photographic image photographed by said camera, and said identification information is at least an identification information of a file name of said photographic image or an identification information of a photographer of said photographic image.

6. (previously presented) The method according to claim 4, wherein said imaging apparatus has a computer, in which said produced image is a computer graphics image produced by said computer or an image which has been image-processed by said computer, and said identification information is at least an identification information of a file name of said produced image or an identification information of a producer of said produced image.

7. (Currently Amended) A method of preventing falsification of a produced image produced in an imaging apparatus, comprising the steps of:

sending authentication data from an authentication section for authenticating a status that there is no falsification in a produced image which is produced by said imaging apparatus to said imaging apparatus~~,~~;

recording said authentication data and identification information for identifying said produced image of said imaging apparatus into a database in said authentication section~~,~~;

attaching said authentication data to said produced image or embedding said authentication data into said produced image, when said imaging apparatus produces said produced image;

requesting authentication of an authentication object image to said authentication section, to which identification information is provided;

reading out said authentication data recorded together with said identification information of said produced image which is the same as said identification information of said authentication object image from said database in said authentication section;

extracting said authentication data attached to or embedded into said produced image from ~~an~~ said authentication object image which has been requested to be authenticated in said authentication section;

comparing said extracted authentication data with said authentication data ~~recorded in~~ read out from said database~~, in which said extracted authentication data and said authentication data recorded in said database have the same identification information,~~; and

judging whether or not said authentication object image is falsified after said image production, based on a consistency between said extracted authentication data and said authentication data acquired from said comparison in order to prevent said falsification of said produced image based on said judgment.

8. (original) The method according to claim 7, wherein said imaging apparatus has a camera, in which said produced image is a photographic image photographed by said camera, and said identification information is an identification information of said camera or a file name of said photographic image or an identification information of a photographer of said photographic image.

9. (original) The method according to claim 7, wherein said imaging apparatus has a computer, in which said produced image is a computer graphics image produced by said computer or an image which has been image-processed by said computer, and said identification

information is an identification information of said computer or a file name of said produced image or an identification information of producer of said produced image.

10. (New) The method according to claim 1, wherein said one specified algorithm is selected from a plurality of algorithms in each photographing session of said produced image in said imaging apparatus.

11. (New) The method according to claim 1, wherein said information of said one specified algorithm is information for selecting said one specified algorithm from a plurality of algorithms in each photographing session of said produced image in said imaging apparatus.

12. (New) The method according to claim 1, wherein said one specified algorithm is confidential.

13. (New) The method according to claim 1, wherein when looking at the consistency the exact matching between the data is not required.

14. (New) The method according to claim 4, wherein when looking at the consistency the exact matching between the data is not required.

15. (New) The method according to claim 4, wherein said first and second image data are entire image data of said produced image and said authentication object image, respectively, compressed image data compressed from said entire image data or thinned-out image data thinned-out from said entire image data.

16. (New) The method according to claim 15, wherein said compressed image data is compressed from said entire image data by using one specified compressing algorithm, or said thinned-out image data is thinned out from said entire image data by using one specified thinning-out algorithm,

said one specified compressing or thinning-out algorithm, or information thereof is recorded together with said identification information for identifying said produced image and said first image data of said produced image into said database in said authentication section, and

said one specified compressing or thinning-out algorithm, or information thereof is read out together with said first image data from said database in said authentication section.

17. (New) The method according to claim 16, wherein said one specified compressing or thinning-out algorithm is selected from a plurality of compressing or thinning-out algorithms in each photographing session of said produced image in said imaging apparatus, respectively.

18. (New) The method according to claim 16, wherein said information of said one specified compressing or thinning-out algorithm is information for selecting said one specified compressing or thinning-out algorithm from a plurality of compressing or thinning-out algorithms in each photographing session of said produced image in said imaging apparatus, respectively.

19. (New) The method according to claim 16, wherein said one specified compressing or thinning-out algorithm is confidential.

20. (New) The method according to claim 7, wherein

said authentication data is watermark information attached to or embedded into said produced image and said authentication object image said photographed image by using one specified attaching or embedding algorithm,

said one specified attaching or embedding algorithm, or information thereof is recorded together with said identification information for identifying said produced image and said authentication data into said database in said authentication section,

said one specified attaching or embedding algorithm, or information thereof is read out together with said authentication data from said database in said authentication section.

21. (New) The method according to claim 20, wherein said one specified attaching or embedding algorithm is selected from a plurality of attaching or embedding algorithms in each photographing session of said produced image in said imaging apparatus, respectively.

22. (New) The method according to claim 20, wherein said information of said one specified attaching or embedding algorithm is information for selecting said one specified attaching or embedding algorithm from a plurality of attaching or embedding algorithms in each photographing session of said produced image in said imaging apparatus, respectively.

23. (New) The method according to claim 20, wherein said one specified attaching or embedding algorithm is confidential.

24. (New) The method according to claim 7, wherein when looking at the consistency the exact matching between the data is not required.